Image Encryption System by Generating Chains from the Secret Key

نظام تشفير الصورة عن طريق توليد سلاسل من المفتاح السري

By

May Fawaz Al -Jabali

Supervisor

Dr. Mohammed A. F. Al Husainy

A Thesis Submitted In Partial Fulfillment of the Requirements for the

Master Degree in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

July , 2016

Authorization Statement

I, **May Fawaz Al -Jabali**, Authorize Middle East University to supply hard and electronic copies of my thesis to libraries, establishments, bodies and institutions concerned in research and scientific studies upon request, according to the university's regulations.

Date: 18 /07/2016

Signature:

Committee Decision

This thesis "Image Encryption System by Generating Chains from the Secret Key" was discussed and certified on July, 2016.

Thesis committee		**Signature**
Dr. Mohammad A. F. Al Husainy	Supervisor	
Dr. Ahmad Kayed	Chairman	
Dr. Ghassan Issa	Member	

Acknowledgment

I knew from the beginning that pursuing graduate study is a difficult and challenging task. Throughout this long journey, I learned how to be persistent on seeking my goals despite hardships. I am grateful for all the support and contribution I got along this journey. I would never have successfully completed this thesis without the assistance of numerous people who I am indebted to. I am forever indebted to my family who supported me at all times; they had more faith in me than could ever be justified by logical argument.

I, also, would like to express my sincerest appreciation to my supervisor Dr. Mohammad A. F. Al-Husainy for his precious thoughtful consideration and guidance. Without his guidance, support and inspiration during the most critical period of my Master degree journey, I would not have been able to accomplish this study. To him, I wish to say ‘You are a wonderful and a great mentor!

Many sincere thanks, also, go to the Information Technology Faculty members at the Middle East University for their insightful instructions and suggestions, thank you for teaching me how to be a dedicated researcher.

Finally, million thanks go to my fellow colleagues for their support and encouragement.

Dedication

{وقُلْ ربِّ زدْنِي عِلْمًا} [طه]111

I would like to express my gratitude to the one who always encourages me to follow my dreams, thanks for believing in me and for listening to my wild ideas for countless hours. Without your constant love and support, this work could not have happened. You are my best. Thank you to the moon and back.

Table of contents

List of tables

List of figures

List of Abbreviations

DES	Data Encryption Standard
AES	Advanced Encryption Standard
SKC	Secret Key Cryptography
ECB	Electronic Codebook
CBC	Cipher Block Chaining
CFB	Cipher Feedback
PKC	Public Key Cryptography
MD	Message Digest
SHA	Secure Hash Algorithm
PSNR	Peak Signal to Noise Ratio
SNR	Signal to Noise Ratio
NMAE	Normalized Mean Absolute Error

Image Encryption System by Generating Chains from the Secret Key

By: May Fawaz Al -Jabali

Supervisor: Dr. Mohammed A. F. Al Husainy

Abstract

Users of Internet daily send and receive many images through social media. These images are vulnerable to hack and tamper by attackers. Therefore, it is necessary to develop methods to protect these images against attackers. In this thesis, a non-traditional encryption method for encrypting images is presented that makes images more protected and secured. The main idea in this work is based on building strong encryption algorithm through implementing the substitution and transposition operations on colors' values of the pixels. These operations are implemented depending on extracted chains from the secret key used in the algorithm. Also, the proposed encryption method uses proportionally large random key (minimum 2048 bits size). This key adds more difficulties in the face of attackers. The required programs have been written to implement the proposed encryption method. Set of numerical (such as Signal to Noise Ratio (SNR), the Normalized Mean Absolute Error (NMAE)), statistical analysis (color histogram) and visual tests have been used to evaluate the proposed encryption method. The comparison results between the proposed method and other well-known encryption methods showed that proposed method can be used effectively to provide good protection for the image.

Keywords: Diffusion, Confusion, XOR operation, Hexadecimal

نظام تشفيرالصورةعن طريق توليد سلاسل من المفتاح السري

اعداد:مي فواز الجبالي

اشراف :د .محمدعباس فاضل الحسيني

الملخص

مستخدمي الإنترنت ترسل وتستلم يوميا العديد من الصور من خلال وسائل التواصل الاجتماعية. هذه الصور هي عرضة للاختراق أو العبث من قبل المهاجمين. وبالتالي، فمن الضروري تطوير طرق لحماية هذه الصور ضد المهاجمين. في هذه الأطروحة، يتم تقديم طريقة تشفير غير تقليدية لتشفير الصور التي تجعل الصور أكثر حماية وأمناً. وتعتمد الفكرة الرئيسية في هذا العمل على بناء خوارزمية تشفير قوية من خلال تنفيذ عمليات إحلال وتبديل على قيم الألوان للبكسل. وتنفذ هذه العمليات اعتمادا على سلاسل مستخرجة من المفتاح السري المستخدم في الخوارزمية. أيضا، يستخدم أسلوب التشفير المقترح مفتاح عشوائي كبير نسبيا (الحد الأدنى 2048 بت حجم). ويضيف هذا المفتاح المزيد من الصعوبات في وجه المهاجمين. تم كتابة البرامج المطلوبة لتنفيذ أسلوب التشفير المقترحة. و قد استخدمت مجموعة من الاختبارات العددية (مثل نسبة الإشارة إلى الضوضاء (SNR)، وخطأ تطبيع متوسط المطلق (NMAE))، التحليل الإحصائي (الرسم البياني للالوان) والاختبارات البصرية لتقييم أسلوب التشفير المقترحة. أظهرت نتائج المقارنة بين الطريقة المقترحة وغيرها من وسائل التشفير المعروف أن الطريقة المقترحة يمكن أن تستخدم على نحو فعال لتوفير حماية جيدة للصور.

الكلمات المفتاحية: الإنتشار، الارباك، وعملية XOR، نظام السادس عشري

Chapter 1: Introduction

1.1 Information Security

Recently, the rapid growth in industrial communications technology and in digital contents leads to the high need of information security. Most of the used applications today need a level of security to be safely used in different communications channels. In addition, the digital information privacy and secrecy of information has become one of the most important issues that force IT experts to develop innovative methods to protect and secure the information. Furthermore, the vast use of networking technology in all over the daily needs makes the information security a significant issue for researchers to propose a new novel technique (Wadi and Zainal, 2014).

To protect secret information against unauthorized users a need has emerged to use various types of encryption methods. (Auyporn and Vongpradhip, 2015). Therefore, it is very important to cipher the multimedia contents that need to be transmitted. So, the Science of Cryptography- image encryption- plays a central role in securing the images sent/received over the mobile phone communications, Pay-TV, e-commerce, sending private emails, transmitting financial information,

security of ATM cards, computer passwords, and touches on many aspects of daily. Cryptography utilizes algorithms in the process of ciphering.

There are two types of Cryptography algorithms*:*

Symmetric Encryption: The symmetric encryption is the oldest and best-known technique. A secret key is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. Examples of symmetric Encryption algorithms are **(**DES, 3DES, AES, and RC4). The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message.

Asymmetric Encryption: this system utilizes two related keys--a key pair. The first one is the public key and it is made freely available to anyone who might want to send someone a message. The second key is the private key which is kept secret, so that only the authorized person knows it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the

same algorithm, but by using the matching private key (Ahmad et al., 2015).

1.2 Problem Statement

Digital images are considered one of the means that are most commonly used over different information networks. Most of these images often include information on a high degree of confidentiality. Attackers always try to steal, cause damage, or use these private images to extort the owner of these images in different bad ways. In addition, the security of digital images has attracted much attention recently.As a result, the need aroused to suggest a strong way to protect these images against different types of attackers, taking into consideration that the rapid development of the internet and the wide applications of multimedia technology enable people to exchange the digital multimedia with others conveniently over the internet.

The conventional cryptosystems such as DES – Data Encryption Standard, AES - Advanced Encryption Standard, and others have been designed to protect textual data but may not be good for multimedia. The use of conventional cryptosystems to encrypt images directly is not suitable for two reason: (a) the image needs more time to encrypt because it is larger in size than text and (b) the decrypted text must be equal to

the original text, but this is not required for images, that is, small distortion in the decrypted image is acceptable by human perception system (Sivakumar and Venkatesan, 2014).

In the encryption algorithms used nowadays, such as AES, DES, 3DES….etc. substitution and transposition processes are done traditionally but do not cover all pixels. Furthermore, the secret key used is not long enough. All that leads to inadequate encryption that lacks complexity and randomness (Chen et al., 2004).

Although many encryption systems have been developed, they have had some setbacks such as the length of the secret key used, which is a major factor. The main problem in many existing encryption systems is the size of the keys used in encryption process. Since the size of the key used is 64-bit or 128-bit which is not long enough to ensure safe images. So, the key plays the major role to achieve the highest degree of security.

In this thesis a solution is suggested by proposing a model (The Proposed Method) which utilizes a good secured key with random generalization with a large size of minimum 2048 bit. Using the proposed algorithm should add a significant improvement and provide a high protection to the encrypted image.

1.3 Objectives

A nontraditional image encryption system is proposed using a large key to protect images that contain confidential information. This method will add a significant value to the image encryption techniques by using a large secured key that makes it difficult to attack. The proposed method objective is to generate a large size key that can achieve the protection and the privacy of images. The proposed method contribution is to use a secret key. This key is divided into blocks. In these blocks a chain is extracted from each cell of the block. This long chain of keys makes the encryption secured and hard to break. In this thesis, a key sensitivity and statistical analysis is used to evaluate the security of the proposed encryption algorithm.

The objectives of the thesis are:

1. To use a relatively large key to enhance randomness and generate chain from a secret key, with minimum size of 2048 bit.
2. To propose an image encryption method that uses untraditional substitution and transposition methods depending on the chain of secret key. This key is large, random and complicated enough to provide a high degree of image protection.

3. To use a non-traditional way of extracting overlapping chains from secret key.

1.4 Methodology

The proposed approach focuses on bmp color image encryption. The pixels of the image are grouped in 16x16 blocks. The encryption process will be done using a secret key, which constitutes a series of bytes which are divided into 16x16 blocks.

The non-traditional idea in this work lies in the process of extracting a related chain from the secret key where the process of encrypting each cell in each image using X-Or substitution and transposition will be performed. This process will be implemented on each cell in each block, in order to reach perfect generation of serial of random keys. By this, the desired target to have the minimum size of key 2048 bit can be achieved and the image will be fully encrypted.

On the other hand, the decryption process on this image will be by inverting the previous steps.The proposed approach will be implemented by writing C# programming language.The resulting outputs will be evaluated using Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), the Normalised Mean Square Error (NAME), and process time.

These measures have been chosen considering their proven credibility in evaluating the encryption ratio and the amount of the data ciphered.

1.5 Motivation

Due to the increase of the use of technology in every aspect of life, i.e. in the fields of communication, transportation, military, medicine, etc., the main item to be transmitted in these fields is the digital image which contains critical information (e.g. Bank swift, military information). Due to this importance, the transmitted digital image became unsecure in the transmission medium because several attackers target these images whenever possible worldwide in different ways. Thus, it is imperative to find modern and enhanced methods to protect these digital images and their contents from any type of attack.

1.6 limitations

In the process of developing and implementing the proposed methodology, some issues have been faced which affected the work:

1. The first limitation is that the encryption is run on images only.
2. The second is that the image must be bmp.

1.7 Scope of work

In this work, a sample of Color images will be used in order to apply the algorithm. These images are of Bitmap type only. The proposed approach aims to provide high speed of encryption method, high complexity, large key size and randomness in order to enhance the performance and lessen the encryption time.

For implementation then, C# tool will be used. On the other hand, Personal Computers will be used for the evaluation process.

1.8 Question of thesis

1. What is the method that sensitive images are secured against attackers?

2. What are the features that a good encryption system must have?

3. How can confusion and diffusion techniques be applied in a nontraditional way to encrypt images?

1.9 Thesis Outline

Chapter two presents the basic principles of cryptography techniques, discusses the state of art literature, reviews studies and the existing techniques related to the field of research in this thesis.

Chapter three presents the methodology and the proposed work.

Chapter four includes a discussion and an analysis of the experimental results, and presents the comparisons between previous techniques of image encryption methods and with the proposed work in this thesis. Finally, **Chapter five** is the conclusion and future work.

Chapter 2: Literature Review

2.1 Principles of Cryptography

Cryptography is a science that studies how to protect the data privacy. It includes many ways to hide information in storage or transit. In addition, cryptography is associated with scrambling images and messages into cipher form (encryption process), then back again to its original form (decryption process). In other words, the encryption is the process to convert the readable information to non-readable data or cipher (Boneh et al., 2004).

In recent studies, cryptography is considered to be a mapping of both mathematics and computer science fields and it is disaffiliated closely with information theory, computer security, and engineering studies (Bibhudendra et al., 2007).

Figure (2.1) below shows the Basic structure of a cryptographic system.

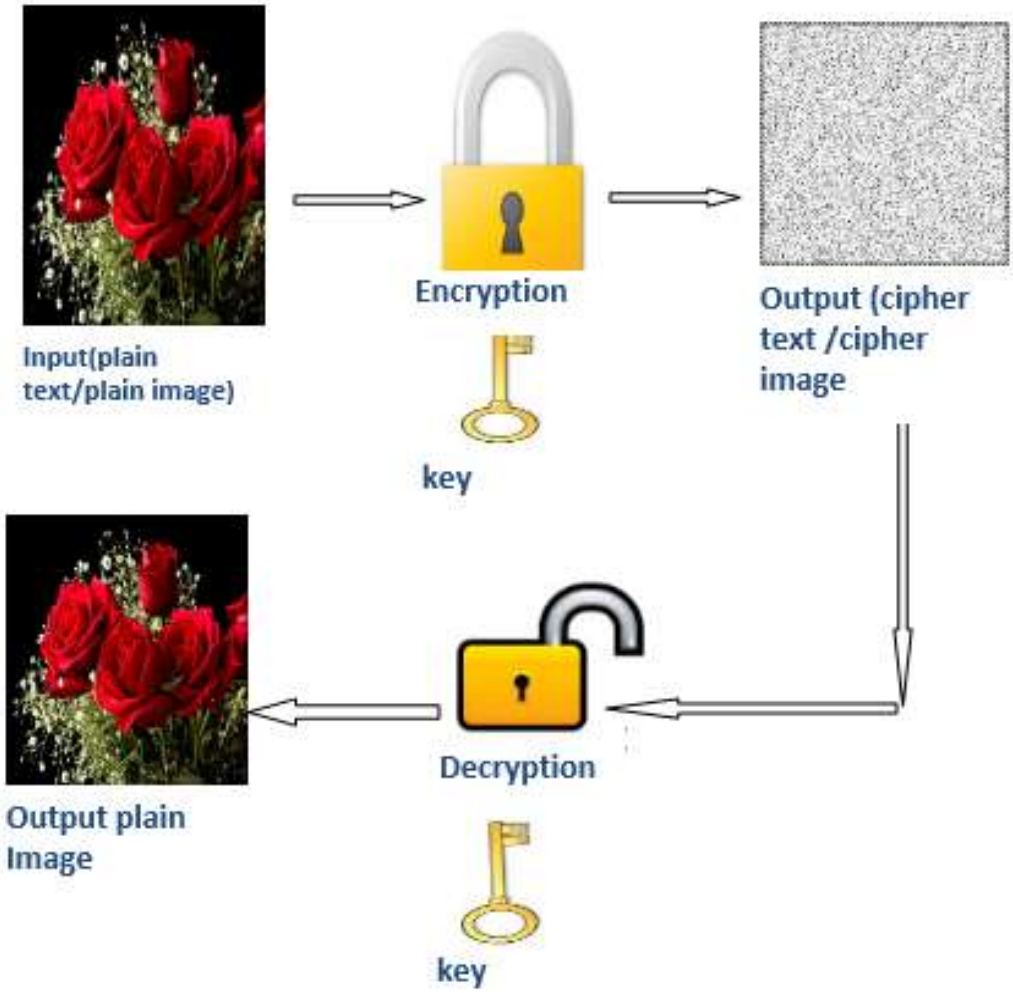


Figure 2. 1: Basic structure of a cryptographic system

2.2 Cryptography Phases

Cryptosystems, in general, consists of two phases: The encryption phase that transforms the original secret data to the coded data, and the decryption phase that transforms back the encrypted data to the original secret data. The keys used in cryptosystems represent the strength of the encryption algorithm. These keys should be complex and large enough

to achieve high security to the secret data. In addition to that, the implementation of the substitution and transposition operations provides enough complexity to produce more and more difficulties to prevent attackers from breaking the encrypted data.

This technique should eliminate the main problem in the existing encryption system that is the size of keys used is not large enough and the keys are less random (Lindner and Piker, 2011).

2.3 Types of Cryptography algorithmscfsvv

The cryptography algorithms can be categorized into three categories based on the number of keys that are employed for encryption and decryption. The three types of cryptography algorithms are presented in the next sections.

2.3.1 Secret Key Cryptography (SKC) or Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. In this system, both the sender and receiver share a single key. This method is also called Secret Key Cryptography (SKC) because a single key is used for both encryption and decryption. A secret key, which can be a number, a word, or just a string of random letters, is applied to the original data to change the content in a particular way. This might be as simple as

shifting each letter by a number of places in the alphabet (Ahmad et al., 2015).

As long as both sender and recipient know the secret key, they can encrypt and decrypt all data using this key. An example of these types of cryptography algorithms are (DES, 3DES, AES, and RC4) (Delfs and Knebl, 2007).The process's steps are shown in Figure (2.2).

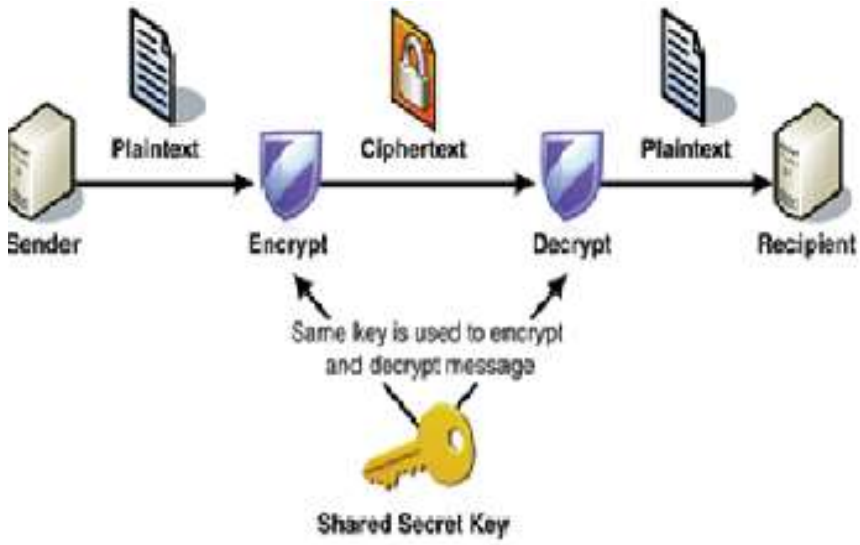


Figure 2. 2: The process of symmetric encryption (Web Service Security, 2005).

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block

cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

2.3.2Public Key Cryptography (PKC) or Asymmetric Encryption

The asymmetric encryption uses two related keys-a key pair.

- A public key that is made freely available to anyone who might want to send you a message.
- The second key is the private key. It is kept secret, so that only one person knows it. Any message (text, binary files, or documents) that is encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). Figure (2.3) illustrates the process of asymmetric encryption and asymmetric decryption (Web Service Security, 2005).

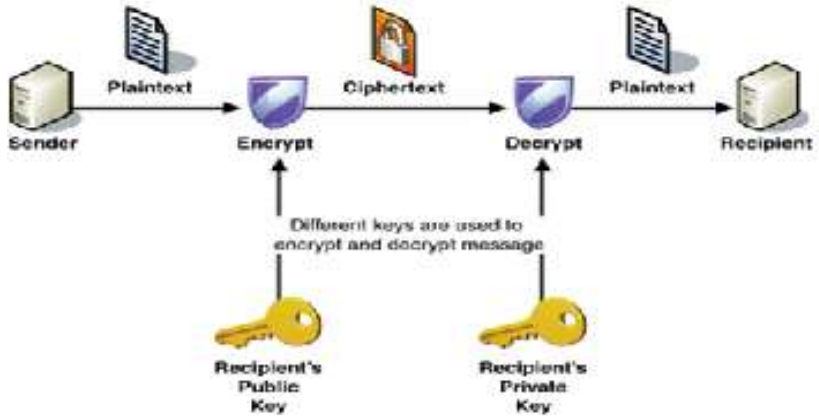


Figure 2. 3: the process of asymmetric encryption (Web Service Security, 2005).

With asymmetric cryptography (also known as public key cryptography), the sender encrypts data with one key, and the recipient uses a different key to decrypt cipher text. The encryption key and its matching decryption key are often referred to as a public/private key pair. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. Examples of Asymmetric Encryption algorithms include (RSA, Daffier-Hellman, Digital Signature, ECDSA, and XTR).

2.3.3 Hash Functions

Cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest (Kaur and Singh, 2012).

There are a number of hash functions types can be used in cryptography. Two series of hash functions MD2, MD4, and MD5, and the Secure Hash Algorithm (SHA), a standard algorithm, that makes a larger (60-bit) message digest and is similar to MD4. These different types of hash functions have different features and shortages.

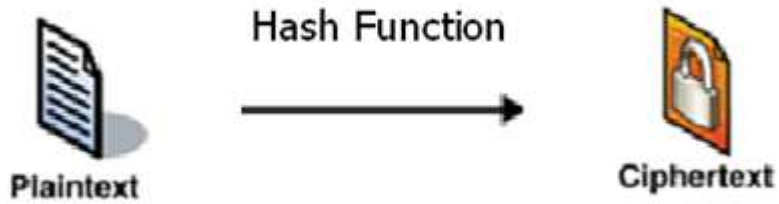


Figure 2. 4: Hash Functions Encryption

Common Hash algorithms include the following:

- Message Digest (MD) algorithms: A series of byte-oriented algorithms that produces a 128-bit hash value from an arbitrary-length message.
- Secure Hash Algorithm (SHA) :the SHA function is hash algorithm in which n-bit hash produces n-bit length finger print from the arbitrary length data. SHA- 1 produces message digest160, SHA-256, SHA-512, (Guo et al., 2010).

2.4 Cryptography Properties

Cryptography provides a number of security properties to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. The most desirable property of any image cryptography is to maximize the strength of the secret key in order not to be hacked and to be secured against detection by unauthorized parties, Figure (2.5) below shows the Cryptography Properties. The following sections show the various goals of cryptography (stalling fourth edition).

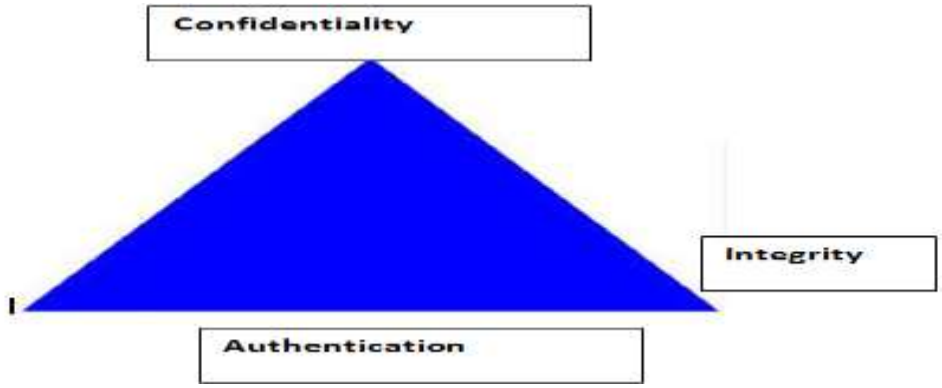


Figure 2. 5: Cryptography Properties

2.5 Image Security

Information security is a major concern in our society these days. Cryptography is a powerful tool to achieve information security. However, o the main challenge in cryptosystems is to maintain the secrecy of the keys.

Image data is highly sensitive and prone to abrupt decoding intruders. In current situation, preserving the security and confidentiality of the image data is a critical issue (Delfs, and kneble, 2007).

Each image is made of small units called pixels. These pixels are aligned in a matrix .Pixels have the same properties of the original image and each pixel represents a small part of the image. When scanning an image by a scanner or a digital camera the image is divided into small pixels in rows and Columns and each pixel are transferred. These pixels are put in

three colors: Red, Green, and Blue when encrypting, upon using substitution and transposition change the original location and number is changed to new order.

The aim of applying image encryption by implementing random multi systems is to increase the key spaces .thus, this key makes breaking the encryption very difficult. However, it has been found the values of calculations and the execution time of encryption are very high .Therefore, apply changes in the pixels value and there position to increase the ambiguity in the cipher image.

It has been established that must of the chaos –based image encryption algorithms are based on confusion and diffusion techniques. Confusion technique shuffles the positions of pixels in plain-image to get visually disordered and unrecognizable image. Diffusion technique alters the statistical characteristics of image by modifying the gray-values of pixel.

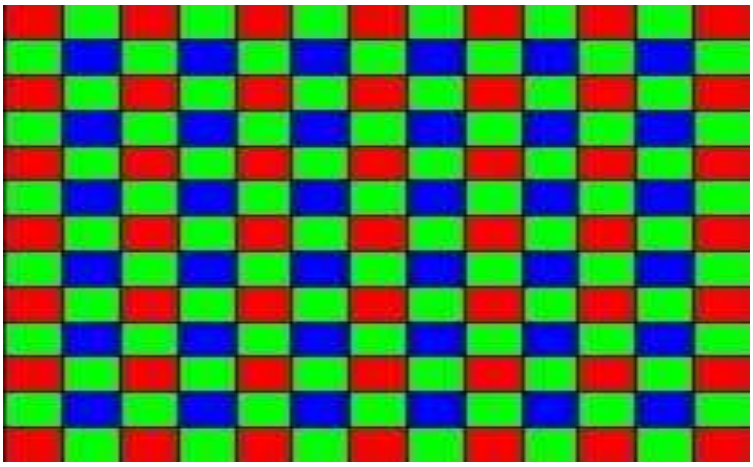


Figure 2. 6: pixel of RGB (www.google.com/digitalcamera)

2.5.1 Image Cryptography and Image Steganography

Cryptography provides transmission of data from one end to another securely and secretly. Cryptographic systems are used very extensively to ensure secrecy and authenticity of sensitive information.

Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient. In any communication, security is an imperative issue in the world today. Many data security and steganography algorithms were created in the past decade, and motivated our research. The system was designed to allow the average user to securely transfer secret messages (picture) by hiding them in a JPEG image file using local characteristics within the image.

2.5.2 Randomness

Random numbers are useful for generating encryption keys, simulating and modeling complex phenomena and selecting random samples from larger data sets. Generation of random numbers consists of two main approaches that are the Pseudo-Random Number Generators (PRNGs) and the True Random Number Generators (TRNGs). Many digital computers are built with inputs that digitize some real world analog sources such as sound from microphone and audio. If the system has enough gain, it can detect anything (SivakumarandVenkatesan, 2016).

2.5.3 Size of key

According to the basic principle of cryptology, a cryptosystem should be sensitive to the key, i.e., the cipher-text should have close correlation with the key. There are two ways to accomplish this requirement: one is to mix the key thoroughly into the plain-text through the encryption process; another is to use a good key that is randomized. A good key is characterized by the length of the key (thronged the better) and the randomness of it.

2.6 Literature Review

Because digital images are the most common way to share information between People, these images, in most times, contain private information. Many researchers in security field exert much more effort

to innovate new non-traditional techniques to achieve strong protection for these images. Many studies and researches were presented in the field of image encryption and decryption techniques. The use of image encryption techniques have increased and become an important issue in how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are proposed from time to time to encrypt the images for more security. Dealing with image encryption techniques will cause scrambling the pixels of the image and decreasing the correlation among the pixels, so that a lower correlation will be gotten among the pixel and get the encrypted image.

Sathish et al., (2011) presented a new image encryption method based on integrated pixel scrambling plus diffusion technique [IISPD]. The proposed algorithm makes use of full chaotic property of logistic map and reduces time complexity. They calculate the permuting address for row and column by the bitwise XOR'ing operation by the adjacent pixel values of original image. The security analysis and its experimental analysis show that the proposed technique is highly sensitive to initial conditions, higher key space, and higher degree of scrambling.

Upon comparing this study whit the [IISPD] the following point were notices methodology as for [IISPD] method the method of ciphering

depends on running semi –traditional X-OR operation with confusion to scramble the neighboring pixels row by row and column by column .two keys are used the KX for rows and KY for columns .by these the ciphered image is obtained as for the proposed method, it uses a series of substitutions XOR transposition operations based on nontraditional .resulting in a change of order in the pixels using long size key.

Measures the [IISPD] method shows a correlation ratio of cipher image (-0.0070493) on the Lena image, while the ratio shows (0.079) .these shows that the value of the correlation ratio of the cipher image is higher in the proposed method which means that the key sensitivity is better in the proposed method .

Wadi and Zainal (2013) presented some modifications to enhance the performance of AES algorithm in terms of time ciphering and pattern appearance especially when the AES use for ciphering the HD images. These modifications have been done by decreasing the number of rounds to one and replace the S-box with new S-box to decrease the hardware requirements.

Chaumont et al., (2013) presented an approach based on a color reordering algorithm after a quantization step. The method protected the color information of an image by embedding it in its corresponding gray

level image. Based on a layer scanning algorithm, the color reordering generates gray level images and makes it possible to embed the color palette into the gray level images using a data hiding algorithm. The structure of the method is shown in. They quantize the original color image, by using the luminance image in order to choose the number of colors. Then, the color reordering algorithm used to get a reordered color palette and an index image close to the luminance image. The last step consists of embedding the color palette (message), in the index image (cover).

Color reordering these method depends on quantizing the original image's colors and put them in correspondent gray scale value using a color index .after that, the resulted color reorder in patterns .

In other word, this technique depends on ciphering the colors rather than the data unlike the proposed method in these study .revising the measures of (PSNR) which taken on different images (each of 256 colors) the flowing values were recorded Lena image size 315×230 PSNR 38.63 db while proposed is 7.05, Baboon image 256×256 33.31 while proposed is 5.491db and Pepper image 256×256 PSNR 36.34 while proposed 5.026db. The values show that the proposed method is more effective considering that it involves ciphering data and colors.

Different technique was proposed by Reader and Salam (2014) who used a selective block encryption technique to achieve the different goals of security such as Availability, Confidentiality, and Integrity. This new proposed Selective Block Encryption algorithm is a block cipher. They divide the data into blocks of pixels of equal length. They select some blocks of pixels and the selected blocks are only encrypted by using a special mathematical set of functions known as key. The used a symmetric key technique for both encoding and decoding. In addition, they improve the algorithm to for strong security by apply the shuffling technique. Besides that, they protect the cipher image from unauthorized access such as Brute-force by applied the selection process and the key was changed many times in the encryption process, but it will be very hard to attain original image from cipher image.

Theses method takes longer time of ciphering due to the shuffling and selection process furthermore these process does not include all pixels of the original image while in the proposed method the series of substation and transposition process in sure that all pixels are ciphered.

Al-Husainy (2012) proposed a new method based on diffusion and confusion effects in the encrypted image. The method is based on mixing the two Boolean operations (transposition and substitution) based on XOR and Rotation the bits of pixels in the image data. The method was

implemented in two phases the first one by a sequential XOR operation on all the bits of pixels in the image, and the second by adding a circular rotate right of the pixels. The proposed method evaluated and analyzed using key space analysis, key sensitivity analysis, and statistical analysis. The proposed method improved the security of the confusion module by using a bit-level permutation method that introduced a diffusion effect with confusion effect.

Sivakumar and Venkatesan (2013) they used a Matrix Reordering (MR) by employing kind of scanning and simple XOR operation to produce a novel approach for encrypting digital images. The MR is used to make a permutation in the pixel positions and the XOR operation is done to diffuse the pixel values. Pseudorandom numbers generated by the linear method have been used to perform the bitwise XOR operation.

In Song and Qiao (2015) study they proposed a novel image encryption scheme based on DNA encoding and spatiotemporal chaos. The DNA mapping rule is introduced to encode the diffused image that is previously generated from the plain image by primarily diffused with the bitwise XOR operation. According to the sequence generated by the spatiotemporal chaotic system, the DNA encoded image is confused again. The spatiotemporal chaotic system is used to confuse the rows and columns of the DNA encoded image to enhance the encryption.

Other research done by Yang et al., (2015) whom found out that quantum walks (QW) can serve as an excellent key generator thanks to its inherent nonlinear chaotic dynamic behavior. They constructed a novel QW-based image encryption algorithm. The researchers studied the potential application of a famous quantum computation model, i.e., quantum walks (QW) in image encryption.

Chang et al., (2001) used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

BaniYounes and Jantan (2008) introduced a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their

results also showed that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

Yun-peng et al., (2009) research focused on the combination of image encryption algorithm like chaotic encryption, DES encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used; it carries on the RGB with this sequence to the image chaotically, and then makes double time encryptions with improvement DES. This algorithm had high security and the encryption speed.

GU and Han (2006) made a new highly optimized image algorithm using permutation and substitution methods. It was done in order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used.

Nag et al., (2011) introduced a new algorithm by using affine transform based on shuffling the image pixels. It was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x2 pixels blocks and each block is encrypted using XOR operation by four 8-bitkeys.The result proves that

the correlation between pixel values was significantly decreased after the affine transform.

Chapter 3: Methodology and the Proposed Technique

3.1 Introduction

In this thesis, proposed a new encryption algorithm based on using proportionally large key size (16 x 16) byte minimum. A set of successive keys of this size are used in the transposition and substitution operations which adds significant protection to the input image. These keys are expected to increase the security of the proposed technique. The transposition operation produces a confusion effect, while the substitution operation produces a diffusion effect in the data image. The diagram of the proposed algorithm is shown in Figure (3.1).

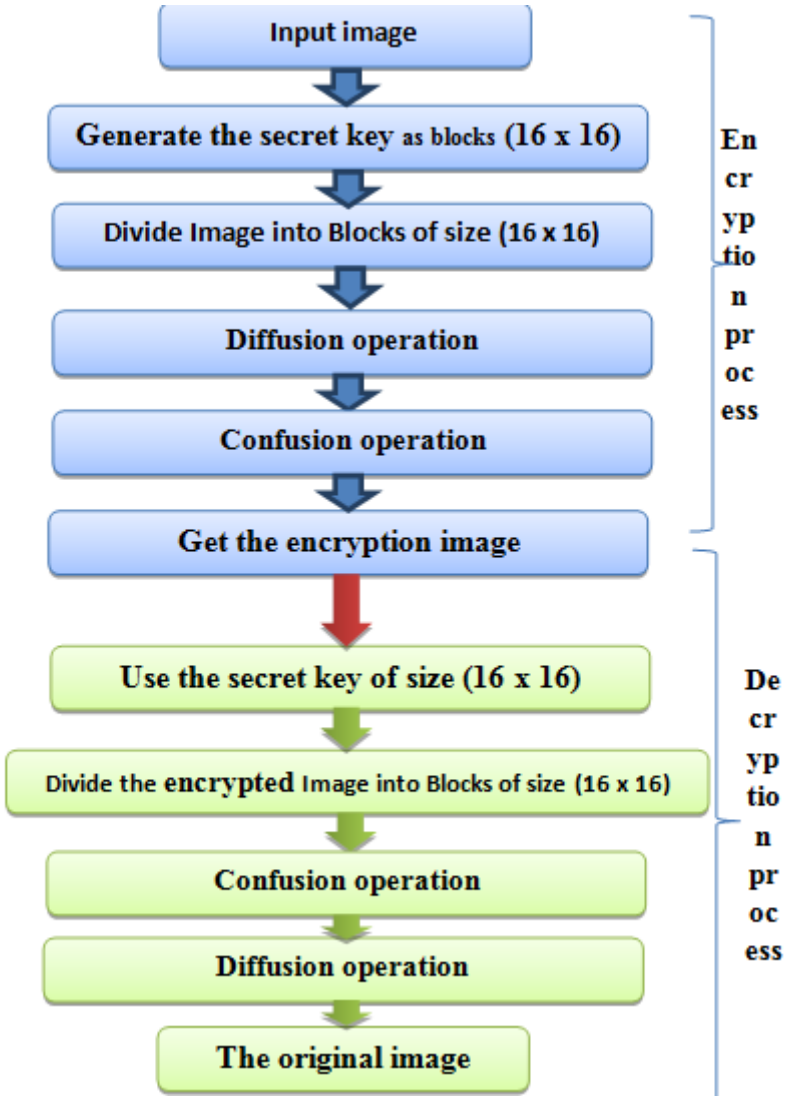


Figure 3. 1: Diagram of the proposed algorithm

3.2 Methodology and the Proposed Work

The idea of the proposed method is to encrypt digital images using a simple transposition and substitution operations to produce a high secure encryption and decryption method. The proposed work will use a proportional large secret key formed as matrix of size (16 x 16) of bytes

(represented in hexadecimal number system). This key used in transposition and substitution operations to satisfying a good confusion and diffusion features in the encrypted image. Since, some of literature studies proved that the confusion module shows a low security levels in image encryption and sometimes it is weak against statistical attacks where the histogram of the shuffled image is unchanged. To improve the confusion weakness and the encryption process, this thesis proposes a bit-level permutation method based on a certain diffusion effect with confusion effect. This is done based on the inactive confusion and diffusion modules based on transposition and substitution operations on the original image. This process is done many times depending on the secret key size; the original image will divided into blocks of size (16 X 16) pixels. The overall methodology diagram is shown in Figure 3.1, the architecture of encryption phase is shown in Figure 3.2 and the architecture of decryption phase is shown in Figure 3.3.

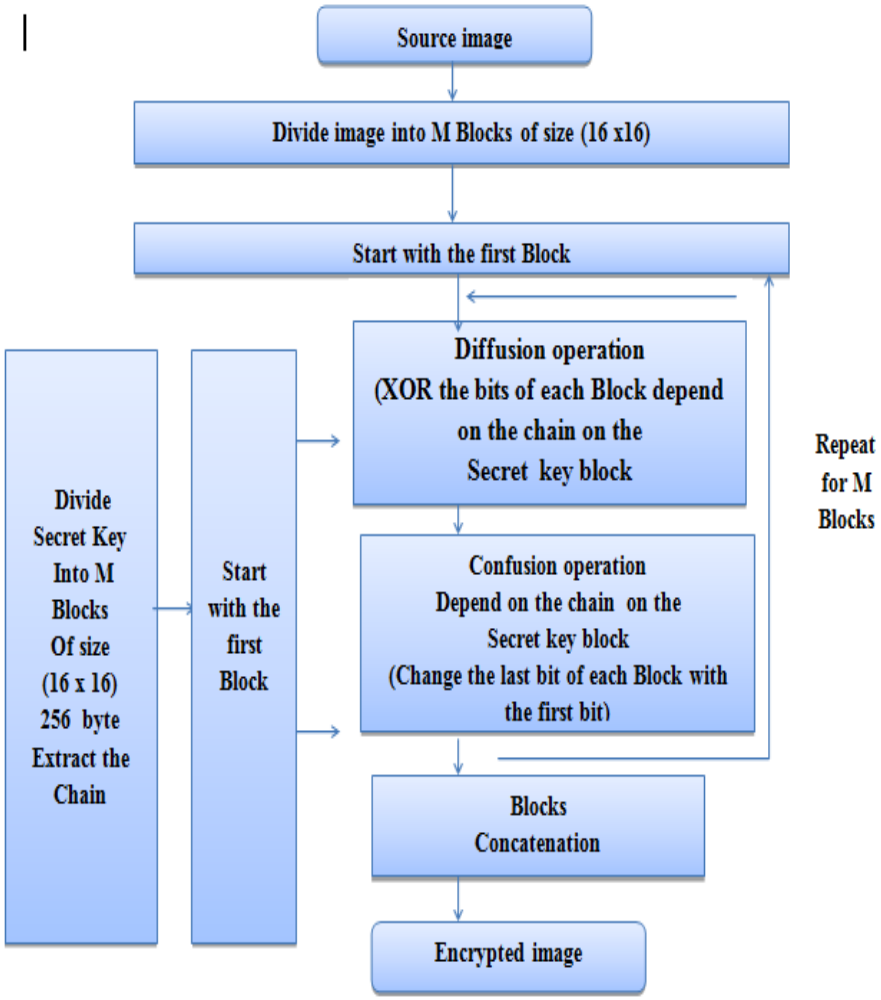


Figure 3. 2: The architecture and the methodology of the proposed encryption phase

Where M blocks is the **Source *image*** $_{size}$ **/ Secret key (16×16)** $_{size}$

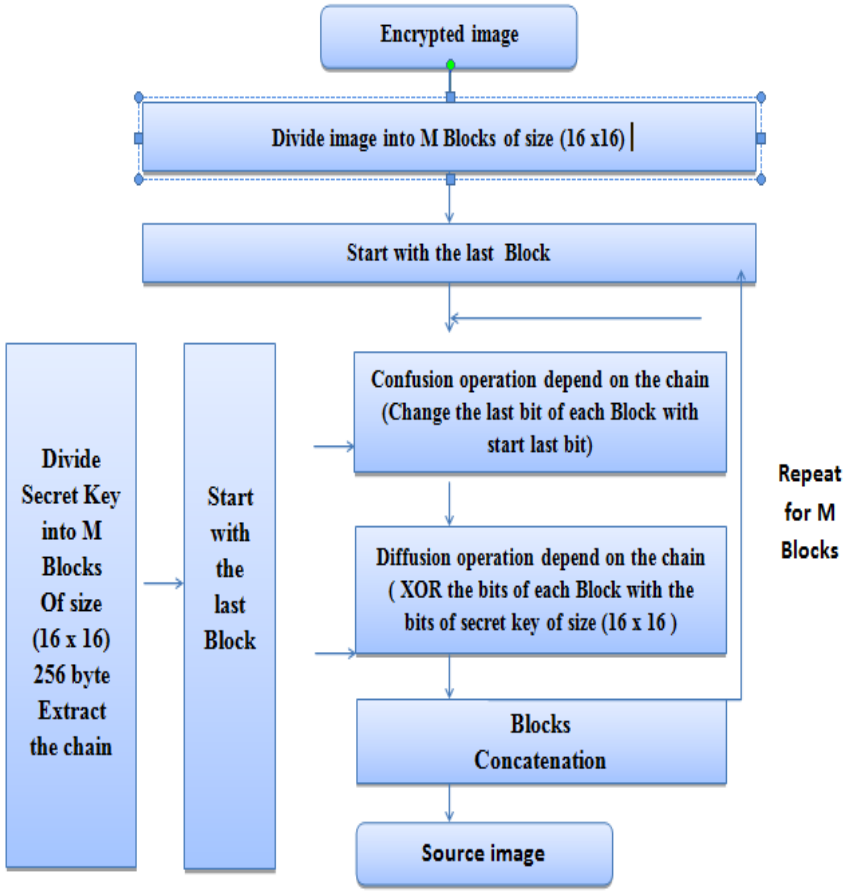


Figure 3. 3: The architecture and the methodology of the proposed decryption phase

Where M blocks is the **Encrypted*image*$_{size}$ / Secrect key (16×16)** $_{size}$

To illustrate the proposed algorithm methodology, the following definitions and terminologies were proposed: **Secret Key (K)**: series of bytes may represent any digital file such as: image, sound, text, etc.

The generation of the secret key is very important in order to achieve good protection for the encrypted data. In addition, the length of the

secret key must be as large as possible and has as random as possible bytes in it.

- **Secret Key Length (Length)**: number of bytes in the secret key K.
- **Original Image (S)**:two-dimensional bitmap image of pixels that has Width, Height, and Palette. The encryption method treats the image's file as a series of bytes, where each value of byte is between (0...255) and (1byte = 8bits).
- **Original image Length (Length)**: number of bytes in the original image S is equal (Width x Height x Palette).
- **Encrypted Image (E)**: the resulting encryption image forms the original image S that is generated after finishing the encryption stage.

Table 3. 1: Sample of data block

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	B9	D1	C4	8E	34	8F	E7	71	FA	46	4A	77	A1	78	FB	7
1	DC	FE	AD	50	D1	D9	FD	8	B3	86	EF	B0	8B	14	2F	74
2	4C	FD	A4	C3	7	61	57	F5	81	B7	1E	46	E8	CB	56	75
3	25	38	68	B7	9E	7C	31	E0	D3	BC	DB	AE	9F	37	E5	E5
4	16	D6	2B	A4	D3	38	FF	7B	A6	B8	CF	19	BA	B7	20	E7
5	30	7A	8A	53	AB	77	D5	CF	CB	C3	F0	4B	85	A9	55	49
6	D2	38	2F	11	9F	B1	A1	ED	38	ED	11	E6	AD	18	26	1B
7	9C	F3	7D	25	AD	91	39	9E	1	5C	D9	F	48	B4	F5	FD
8	63	85	47	81	88	E	47	7E	D8	9C	1A	BE	66	EE	21	B3
9	9D	D4	AF	91	2C	2F	9B	40	FF	91	10	43	D7	91	A5	84
A	F8	13	83	27	D0	A4	93	8D	AC	FE	4D	10	77	7B	37	12
B	3A	26	72	73	5	63	D0	33	E9	7	82	F6	FE	4	A7	47
C	F7	96	C5	52	6B	F9	E2	F9	41	21	E5	2D	E2	8B	C8	83
D	5A	FD	8	B1	1F	31	7F	94	42	4F	3D	C8	22	9C	8F	A7
E	57	5	18	E0	B5	E4	A6	41	43	79	32	E3	7D	A3	51	5E
F	3E	FE	9C	0	FB	F6	28	C5	17	30	10	1C	BB	1A	D6	A4

- **Decrypted Image (D)**: the resulting decryption image from the **E** image that is generated from encrypted image E.

- **XOR Boolean Operation**: Boolean operation which uses in the encryption and decryption phases to make changes in the bits of the series bytes of the image.
- **Secret Key Block (KB)**: it is a two dimensional matrix secret key of the size (16 x 16). The bytes in the secret key matrix represent a set of 256 bytes from the secret key the bytes values in this matrix are represented in hexadecimal number system. Table 1: shows an example of (16×16) Secret Key Block KB.

Table 1: Example of (16×16) Secret Key Block KB.

- **KB (i, j)**: represents a byte at row i and Colum n j in KB.
- **ImageDataBlock (DB (b))**: represents a two-dimensional matrix of size (16 x 16) of the original image. Bytes of **DB (b)** represents a set of bytes from original image S (in encryption stage) or encrypted image E (in decryption stage).
- **DB (b, i, j) :** represents a byte in block b at row i and column j.
- **NextElement:** represents a two-dimensional matrix of pair of indices (r,c), each pair represents the row r and the column c of the next element in the matrix. The determination of what the next element is based on the corresponding element's value in KB.

The following situations will appear when scan the matrix elements (row by row) from the element (0, 0) to (15, 15):

- If KB (i, j) was not chosen as a next element previously and KB (i, j) = XY, where X and Y are the left and right digits of the hexadecimal value of the element KB (i, j). This means that the pair that is set in the NextElement (i, j) =(X, Y).
- If KB (i, j) was chosen as a next element previously. This means that the pair that is set in the NextElement (i, j) =(i, j). (i.e., there is no next element to the element (i, j))

The elements' chains for some selected elements in the above Next Element matrix are:

- **[0,0]**-(B,9)-(0,7)-(7,1)-(F,3)
- **[0,2]**-(C,4)-(6,B)-(E,6)-(A,6)-(9,3)-(9,1)-(D,4)-(1,F)-(7,4)-(A,D)-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)
- **[1,8]**-(B,3)-(7,3)-(2,5)-(6,1)-(3,8)-(D,3)-(B,1)-(2,6)-(5,7)-(C,F)-(8,3)-(8,1)-(8,5)-(0,E)-(F,B)-(1,C)-(8,B)-(B,E)-(A,7)-(8,D)-(E,E)-(5,1)-(7,A)-(D,9)-(4,F)-(E,7)-(4,1)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)
- [**1,9]**-(8,6)-(4,7)-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)

- **[8,9]**-(9,C)-(D,7)-(9,4)-(2,C)-(E,8)-(4,3)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)
- **[8,A]**-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)-(D,6)-(7,F)-(F,D)
- **[A,D]**-(7,B)-(0,F)-(0,7)-(7,1)-(F,3)-(0,0)-(B,9)
- **[A,E]**-(3,7)-(E,0)-(5,7)-(C,F)-(8,3)-(8,1)-(8,5)-(0,E)-(F,B)-(1,C)-(8,B)-(B,E)-(A,7)-(8,D)-(E,E)-(5,1)-(7,A)-(D,9)-(4,F)-(E,7)-(4,1)-(D,6)-(7,F)-(F,D)-(1,A)-(E,F)-(5,E)-(5,5)-(7,7)-(9,E)-(A,5)-(A,4)-(D,0)-(5,A)-(F,0)-(3,E)-(E,5)-(E,4)-(B,5)-(6,3)-(1,1)-(F,E)

3.2.1 Encryption Phase Algorithm

The algorithm creates the encryption image **E** from the source image **S**; the following steps clarify in details the operations in this phase of the proposed method.

The proposed encryption method has the following steps:

- **Step1:** Read (from the user) the secret key $\boldsymbol{K}$ of length $\boldsymbol{K_{Length}}$.
- **Step2:** Read (from the user) the original image $\boldsymbol{S}$ of length $\boldsymbol{S_{Length}}$.

- **Step3:** Represent the original image ***S*** as ***m*** number of blocks ***DB*** of size (16×16). Where: $M = S_{Length} / (16 \times 16)$and the set of blocks are: $DB(0)$ ... $DB(m-1)$
- **Step4:** Set $K_{index} = 0$ and
- **Step5:** For each data block***DB*** from $b=0$ to $m-1$

  (a) Read sequentially 256 bytes from the secret key ***K***and fill ***KB***,(i.e., $K(K_{index})$ ... $K(K_{index}+256)$). When $K_{index} = K_{Length}$ (end of the secret key), then set $K_{index} = 0$ (return to the beginning of the secret key).

  (b) For each element in data block from $DB(b, 0, 0)$ to $DB(b, F, F)$

  1) Build ***NextElement*** Block matrix.

  2) Perform the diffusion substitution operation by **XORing** the corresponding bytes in the $DB(b)$ based on the sequence of elements in the ***Next Element*** matrix. For the above example in Table 1, the value of $DB(b, 0, 0)$ is coring with the key values as follow: Assume the value of $DB(b, 0, 0) = 6E$.

DB*(*b*, 0, 0)**=DB*(*b*, 0, 0)** XOR ***KB*(0,0)**	**1101 0111=0110 1110 XOR1011 1001**
DB*(*b*, 0, 0)**=DB*(*b*, 0, 0)** XOR ***KB*(B,9)**	**1101 0000=1101 0111 XOR 00000111**
DB*(*b*, 0, 0)**=DB*(*b*, 0, 0)** XOR ***KB*(0,7)**	**1010 0001=1101 0000 XOR 01110001**
***DB*(*b*, 0, 0)** = ***DB*(*b*, 0, 0)** XOR ***KB*(7,1)**	**0101 0010=1010 0001 XOR 11110011**
***DB*(*b*, 0, 0)** = ***DB*(*b*, 0, 0)** XOR ***KB*(F,3)**	**0101 0010=0101 0010 XOR 11110011**

3) Perform the confusion operation by **exchanging** the corresponding bytes in the ***DB* (*b*)** based on the sequence of elements in the ***Next Element*** matrix. For the above example in Table 1, the value of ***DB*(*b*, 0, 0)** is exchanging with the values as follow:

***DB* (*b*, 0, 0) ⇨*DB* (*b*, B, 9)**

***DB* (*b*, B, 9) ⇨*DB* (*b*, 0, 7)**

***DB* (*b*, 0, 7) ⇨*DB* (*b*, 7, 1)**

***DB* (*b*, 7, 1) ⇨*DB* (*b*, F, 3)**

- **Step6:** Construct the encryption image ***E*** from the set of the encrypted data blocks.

3.2.2 Decryption Phase Algorithm

This algorithm will regenerate the source image **S** from the encrypted image **E**; the following steps clarify in details the operations in this phase of the proposed method.

The proposed decryption method has the following steps:

- **Step1:** Read (from the user) the secret key ***K*** of length.
- **Step2:** Read (from the user) the encrypted image ***E*** of length.
- **Step3:** Represent the image ***E*** as ***m*** number of blocks ***DB*** of size (16×16). Where: $M = L_{ength} / (16 \times 16)$
- and the set of blocks are: ***DB*(*0*)** ... ***DB*(*m*-1)**
- **Step4:** Set $K_{index} = 0$ and
- **Step5:** For each data block***DB*** from ***b*=0** to ***m*-1**

  (a) Read sequentially 256 bytes from the secret key ***K***ind fill ***KB***, (i.e., $K\ (K_{index})\ ...\ K\ (K_{index}+256)$). When $K_{index} = L_{ength}$ (end of the secret key), then set $K_{index} = 0$ (return to the beginning of the secret key).

  (b) For each element in data block from ***DB*(*b*, 0, 0)** to ***DB*(*b*, *F*, *F*)**

    1) Build ***NextElement***Block matrix.

2) Perform the diffusion operation by **exchanging** the corresponding bytes in the ***DB(b)*** based on the sequence of elements in the ***NextElement*** matrix.

3) Perform the confusion operation by **XORing** the corresponding bytes in the ***DB(b)*** based on the sequence of elements in the ***NextElement*** matrix.

- **Step6:** Construct the source image ***S*** from the set of the decrypted data blocks.

3.3 Measurements used to evaluate the proposed algorithm

Number of comparison tests on different images was performed by using the proposed encryption system with Data Encryption Standard (DES) and Advanced Encryption Standard (AES). During these tests, measurements such as Signal to Noise Ratio (***SNR***), Peak Signal to Noise Ratio (***PSNR***), Normalized Mean Absolute Error (***NMAE***), and Time of Encryption (***Time***) have been used to check the performance and the quality level of protection that the system can achieve.

3.3.1 Image Histogram

An image histogram is a graphical representation of the pixel intensity distribution of an image. Therefore, an image histogram provides a clear illustration of how the pixels in an image are distributed by plotting the number of pixels at each intensity level.

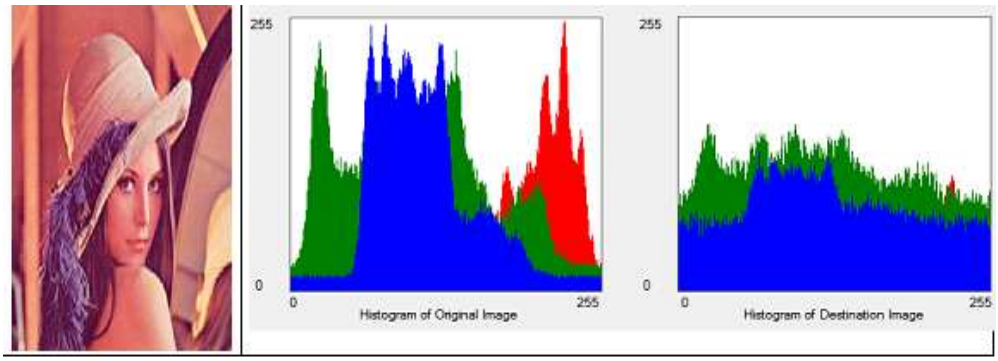


Figure 3. 4: Histogram Red Green Blue

3.3.2 Peak Signal to Noise Ratio (PSNR)

It is one of the measurements of quality between the original image and distorted image. PSNR value represented in a single number measured in the unit of decibels. It is one of the best methods in image processing analysis that measures the ratio of the original data with the distortion (noise) data in the encrypted image. Low PSNR refers to the efficiency of the algorithm of the encryption system.considering the numbers obtained it is noticed that the difference between them are in value in tenths. It is established earlier that these numbers represent the ratio and

the amount of data encrypted. Thus, any small change in the numbers result in big change in the encryption results.

Chapter 4 Experimental Results

4.1 Implementation

The encryption and decryption algorithms were implemented using C#. The experiments are done using a bit mapped (BMP) images that have different sizes with 256 colors.

To evaluate the encryption/decryption processes on the images, different images and different secret keys have been used. The result analysis is carried out for four different samples of images and four different secret key. The Evaluation of results depends on visual evaluation of histogram of the image along with standard evaluation using standard measures such as Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio(SNR), Normalized Mean Absolute Error(NMAE), and time of the encrypted and decrypted image.

To get the value of the ***PSNR*** the following equations is used:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

As for the NMAE ***the*** following equations is used***:***

$$\mathbf{MAE} = \frac{1}{n} \sum_{i=1}^{n} |f_i - y_i| = \frac{1}{n} \sum_{i=1}^{n} |e_i| .$$

4.2 System specification used

Computer system of the following specification has been used to implement and test the proposed image encryption method in this work:

- PC with core i7
- HD 0.5TB,
- RAM 4.00 GB,
- HD Graphic VGA
- Windows 7 professional, 64bit.

4.3 The Expected results

By running the experiment using the aforementioned four images with different sizes type (.bmp) as shown in Table 4.1 below.

Table 4. 1: Images used in experiments

				
Name	**Lena**	**Baboon**	**Pepper**	**Balloon**
Size	**128*128**	**128*128**	**128*95**	**128*128**

In figure 4.1, 4.2, 4.3,4.4 the four images are shown a histogram results of encrypted sample Image which apply on proposed technique.

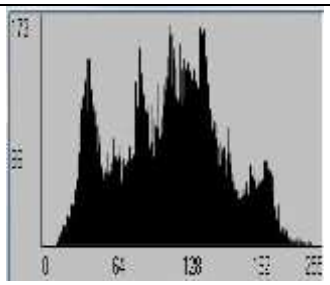
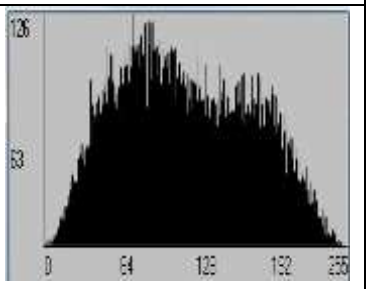
Lena	Original histogram	Encrypted histogram
		

Figure 4. 1: Lena image histogram (Original & Encrypted)

The lena image shows high data image, yet it was highly encrypted and most of the original image processed.

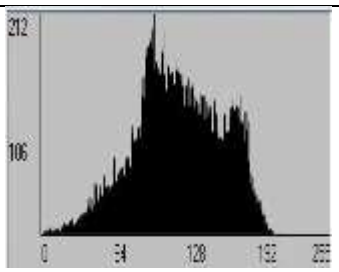
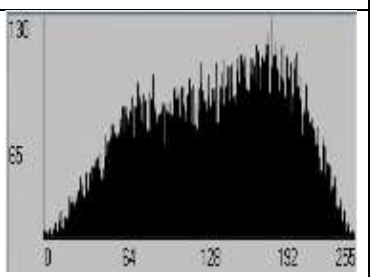
Baboon	Original histogram	Encrypted histogram
		

Figure 4. 2: Baboon image histogram (Original & Encrypted)

The baboon image shows high data image, yet it was highly encrypted and most of the original image processed.

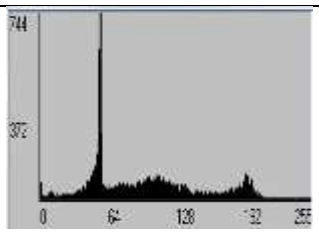
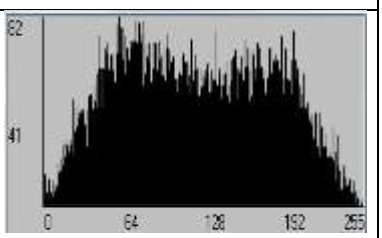
Pepper	Original histogram	Encrypted histogram
		

Figure 4. 3: Pepper image histogram (Original & Encrypted)

In the above histogram it is clearly noticed that the encryption highly achieved by reducing most of the data and increasing the cyphered signal. This proves the power of encryption. Even though that the original data is relatively small in size.

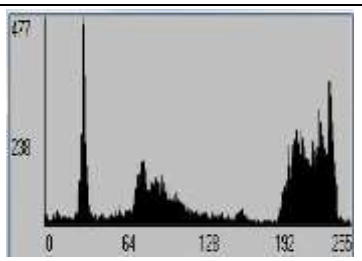
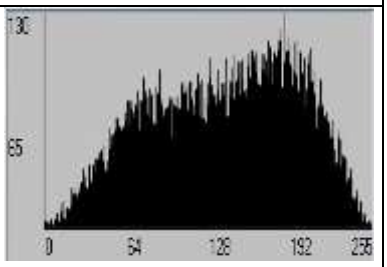
Balloon	Original histogram	Encrypted histogram
		

Figure 4. 4: Balloon image histogram (Original & Encrypted)

The balloon image histogram shows high data image, yet it was highly encrypted and most of the original image processed.

4.3.2 The Result of the Proposed Experiment

Table 4. 2: Proposed technique result

Image	Secret key	SNR (db)	PSNR (db)	NMAE (%)	TIME(sec)
Lena	**Text(27.4)KB**	1.822	7.075	62.839	0.545
Baboon	**Audio(4.61)KB**	2.760	7.618	62.143	0.958
Pepper	**Image(4.19)KB**	0.016	4.899	103.253	0.402
Balloon	**Pdf (1.09)MB**	1.251	5.397	60.307	0.745

In table 4.2 above, it is noticed that there is a direct relation between the secret key file used and the results obtained noticing that the size of all images is kept fixed (up to 128), to eliminate the effect of size on the results obtained. It should be noticed that the performance of the image security dependence on the size of the key and the number of blocks which generated chain of secret key which can be found by the following formula:

16*16*8 x number of blocks

of using the audio secret key on (size 4.61 Kb) on baboon image with 4.61*1024/256 = 18 (approximately) that produced which produces a

(18*2082 = 36864 bit (approximately) however when using the text file 27.4*1024/256 = 109 blocks that produces 109*16 = 223232 which produces SNR = 2.329 db. with 530sec compare to 2.760 with 0.958sec which means a very high difference in cipher baboon image.

Referring to figure 4.3 which shows that data is little compare to Figure 4.1 and figure 4.2 the ***PSNR*** values shown in the table it is noticed that using the image key resulted the lowest value of all while Bothe the text and audio keys resulted the highest Value.

As for the ***NMAE*** values it is shown that the image secret key has exceeded 100% while the other keys show lower value almost (62. %).

The time of each key showed distinctive change that it showed allow value (0.402 sec) for The image smile as a key, while the audio key as a key took (0.938sec) in time _ the Highest value. As for the Time is notice that the pepper image is the less while the baboon has the highest time.

For more elaboration two secret keys have been used on the pepper image to see if changing the key affects the encryption process the results obtained in table (4.3) below.

Table 4. 3: Using two different keys on the Baboon image

The Secret Key	Time (sec)	SNR (db)	PSNR (db)	NMAE (%)
Image (4190) byte	0.527	2.785	7.721	61.274
Audio (4720) byte	0.958	2.760	7.618	62.143

Table 4. 4: Number of blocks in secret key

The Secret Key	Size (byte)	Number of blocks
Image	4190	16
Audio	4720	18

In the table above, the number of blocks for the image is 16 blocks with a size of 4190 bytes which gives 32768 key sizes comparing to the audio (18 blocks, 4720 bytes, 35864). The numbers show that the image has better performance regarding time because it is less in blocks however SNR and PSNR and NAME showed stronger ciphering in baboon image duo to larger number of blocks which lead to increase in number of chains longer secret key that achieve high performance in security.

Table 4. 5: Using two different keys on the Lena image

The Secret Key	Time (sec)	SNR (db)	PSNR (db)	NMAE (%)
Pdf(1.9) Mb	0.601	2.172	7.269	61.254
Text (27) Kb	0.958	2.760	7.618	62.143

In the table above, the number of blocks for the pdf (1.9*1024*1024/256 = 4464). That produces a size of key = 4464*2084 bit which is longer than the text. That shows that high size formed in the result of measures SNR 2.172 less than 2.760 with PSNR 7.269 less than 7.618 in 449 db. That led to more chaos in image achieving high performance of randomness of key and complexity that provides high security.

Table 4. 6: Using two different keys on the Balloon image

The Secret Key	Time (sec)	SNR (db)	PSNR (db)	NMAE (%)
Pdf(1.9) Mb	0.745	1.251	5.397	60.309
Text (27) Kb	0.577	1.97	5.866	58.86

4.3.2 AES Result

Table 4. 7: AES result

Image	SNR (db)	PSNR (db)	NMAE (%)	TIME(sec)
Lena	3.922	8.03	62.436	0.166
Baboon	4.23	7.465	64.465	0.100
Pepper	1.832	6.494	104.011	0.96
Balloon	2.084	6.853	65.695	0.075

The ***AES*** technique is powerful tool of ciphering due to the powerful algorithm in corroborated .if the result obtained from other techniques approach these result then it will be credibility to the techniques .referring to the table 4.7 the following notes are:

The ***SNR*** the pepper image is the less while the baboon is the highest**.**

The **PSNR** Lena image is the highest while the balloon is the lowest**.**

As for the ***MANE*** the highest is pepper image .while lowest Lena image.

4.3.3 DES result

Table 4. 8: DES Result

Image	SNR(db)	PSNR(db)	NMAE (%)	TIME (sec)
Lena	3.887	7.981	62.753	0.207
Baboon	4.238	7.461	65.006	.097
Pepper	1.841	6.488	104.003	0.70
Balloon	2.04	6.815	66.352	0.076

Referring to the above table, the SNR value is higher in the balloon while lower in the pepper as for the PSNR it is higher in the Lena and lowers in the balloon, as for the NMAE is higher in the pepper and lower in Lena.

4.5 Comparison among Technique

4.5.1 SNR db

Table 4. 9: SNR in Proposed, AES and DES

Image	Proposed	AES	DES
Lena	1.822	3.922	3.87
Baboon	2.76	4.23	4.238
Balloon	1.251	2.084	2.04

In the table above the values of the SNR are much better in the proposed techniques than the other techniques referring to the results obtained from the balloon image it has 192 blocks which has been ciphered on 4464 blocks also, considering that data contains in the balloon image affect the outcome which shows difference between the proposed algorithm and AES, DES lies in the favor of the proposed system. These difference (.833) means that chaos in the image is more than the other systems.

4.5.2 PSNR db

Table 4. 10: PSNR in Proposed, AES and DES

Image	Proposed	AES	DES
Lena	7.075	8.03	7.981
Baboon	7.618	7.465	7.461
Balloon	5.397	6.853	6.815

The value of the PSNR is directly related to SNR values explained in table 4.10 and evidently the values of PSNR in the table are lower for the proposed technique than the other two techniques.

4.5.3 NMAE

Table 4. 11: NMAE in Proposed, AES and DES

Image	Proposed	AES	DES
Lena	62.839%	62.436%	62.753%
Baboon	62.143%	64.458%	65.006%
Balloon	62.307%	65.465%	66.352%

In the NMAE variant values shown in table 4.11.it is evident that the ratios in the three techniques are almost the same .That shows that the proposed system is as power full As the AES, DES algorithm techniques.

Furthermore, to prove the efficiency of the proposed technique versus DES, AES Images with different sizes are to be subjected to encryption using the three algorithm techniques .The results are shown in the tables 4.10, 4.11

Table 4. 12: Sizes of images and secret keys

Image	Lena	Baboon	Pepper	Balloon
Size image	250*265	200*128	640*480	200*200
Secret key	Text file 27.kb	Audio 48.kb	Image 4.19 kb	Pdf 1.09 Mb

Table 4. 13: Comparison results between Proposed and AES with different sizes images

	PROPOSED				**AES**			
Source Image	**SNR db**	**PSNR Db**	**NMAE %**	**TIME sec**	**SNR db**	**PSNR db**	**NMAE %**	**TIME Sec**
Lena	1.882	7.05	62.66	1.92	3.878	7.669	63.139	0.35
baboon	1.11	5.419	62.06	0.498	2.672	6.842	65.999	0.70
pepper	0.937	5.026	62.623	0.498	1.895	6.561	61.662	0.88
balloon	2.556	7.438	60.532	5.382	3.93	8.481	63.378	0.35

Looking at the data in the above table it is found that the values obtained when applying the proposed technique are better than AES algorithm technique which support the notion previously mentioned that the proposed algorithm technique is power full and reliable

Table 4. 14: comparison results between Proposed and DES with different sizes of images

	PROPOSED				DES			
Source Image	**SNR db**	**PSNR db**	**NMAE %**	**TIME sec**	**SNR db**	**PSNR Db**	**NMAE %**	**TIME sec**
Lena	1.882	7.05	62.66	1.92	3.894	7.68	63.114	0.511
baboon	1.11	5.419	62.06	0.498	2.076	6.836	66.189	0.78
pepper	0.937	5.026	62.623	0.498	1.858	6.52	62.101	0.81
balloon	2.556	7.438	60.532	5.382	3.989	8.515	63.123	0.319

Also, looking at the data in the above table it is found that the values obtained when applying the proposed technique are better than DES algorithm technique which support the notion previously mentioned that the proposed algorithm technique is power full and reliable despite the change in the size of the images.

4.6 Compare with previous studies

A comparison between these thesis and **A Novel Encryption Method for Image Security** Mohammed Abbas Fadhil Al-Husainy to evaluate the performance of the proposed system .

Table 4. 15: images size used to compare

Name	Baboon	Balloon	Lena	Pepper
				
Size image	128x128	128x128	128x128	128x95

To get results out of comparing between the two studies we used the size of a standard 48.0-bit image that appear in Table 4.13.

In this study, the secret key used to encrypt the image by shuffling each vector with a neighboring vector through diffusion operation Xor and then rotate the new vector right circular rotate) of each vector . Unlike the proposed method which contains a series of operations on o pixel to

pixel basis. This result in that the proposed method ensures that all pixels are processed with non-traditional substitution/transposition operations using long secret key which ensures high security with better efficiency as shown in the following tables

Table 4. 16: SNR between proposed and previous study

Image	Proposed	AL-Husainy
Baboon	2.76	4.1776
Balloon	1.251	2.0713
Lena	1.822	3.8395
Pepper	0.016	1.7691

The SNR values show better performance for the proposed method due to that the ciphered data is more than the other model

Table 4. 17: PSNR between proposed and previous study

Image	Proposed	AL-Husainy
Baboon	7.618	8.7697
Balloon	5.397	6.8326
Lena	7.075	8.6214
Pepper	4.899	6.5778

Also, the above values show that ciphering in the proposed method is stronger.

As a conclusion, it is evident that the technique of the proposed method is more reliable due to the long secret key and its complexity and randomness.

4.7 Security Analysis and discussion

To evaluate the proposed encryption method, many experiments were done using three bitmap images of type (.bmp) which have different sizes. Some security analysis has been performed on the proposed image encryption method, including the most important ones like key space analysis, key sensitivity analysis, and statistical analysis, to demonstrate that these proposed method has good security features.

4.7.1. Experimental Results and Security Analysis

Security analysis was run on the proposed algorithm technique, including the key space analysis, key sensitivity analysis, and statistical analysis, to prove that the proposed method has good security characteristics.

4.7.1.1 Key Space Analysis

The key space is the major factor to determine the robustness of ciphering. Key space can be found using al following formula:

$$16*16*8* k$$

Were 16*16 is the size of the block

8 is the pallet of color red green and blue

K number of blocks which can be found by size of the secret file /256

The series of operations generated chains large space key that provide an adequate complexity and randomness to ensure high quality chaos to the image.

4.7.1.2 Key Sensitivity

To examine the key sensitivity feature of the proposed algorithm technique, a change in one bit is made in the secret key and used afterwards to decrypt the encrypted image. The decrypted image with the wrong key is completely different when it is compared with the decrypted image by using the correct key as shown in Figure (4.5). So, it is established that the proposed encryption method is highly sensitive to the key in a way that even an almost perfect guess of the key does not reveal any information about the plain image.

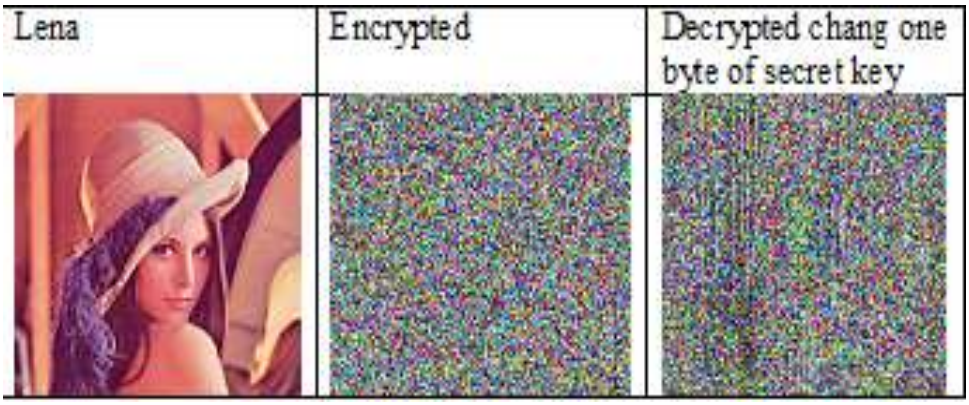


Figure 4. 5: Decrypted Lena image using wrong key

4.8 Robustness and level of security

4.8.1 Robustness

The proposed algorithm technique has proven powerful due to the long key incorporated in the system due to forming chains of elements that change in place and value causing overlapping**.**

4.8.2 Security image

Image encryption method prepared information that are unreadable, therefore, no unauthorized person have access to original image or any other type of transmitting information through public networks. The system ensures privacy and protection solidly**.**

Chapter 5: Conclusion and future work

5.1 Conclusion

In this thesis, a new algorithm was proposed where a significant value was added to the proposed image encryption technique. The algorithm proposed an image encryption method that uses a chain of generated secret key of minimum size of 2048 bit (16*16*8); so, the source image has a series of pixels that are divided into blocks of serial bytes. A series of non-traditional substitution and transposition processes were run on pixel by pixel basis generating a long, complex, and random secret key. This makes the encrypted image very protected. The proposed encryption algorithm uses bitmap images effectively.

In this thesis, the proposed model was experimented on four images (Lena, baboon, pepper, and balloon). The aim was to examine the strength of the secret key. Four measures were used as follows:

1. Signal of original data to the distorted encrypted data (the lower the SNR value is, the better encryption), the results showed:
    - Proposed: from 0.016db to 2.76db.
    - AES: from 1.844db to 3.922db.
    - DES: from 1.844db to 4.258db.

2. (SNR values in the proposed method show better value than AES, DES). The Peak Signal to Noise Ratio (PSNR) - it is a ratio that shows the PSNR, as SNR (the less than value of PSNR, the better encryption got). The values showed:

    - Proposed: from 4.899 to 7.075
    - AES: from 6.494 TO 8.03
    - DES: from 6.488 to 7.981

3. The Normalized Absolute Mean Error (NAME): It is the measure of the encrypted data in a way that the higher the NAME value is, the better encryption. The obtained results showed:

    - Proposed = from 103.253% to 62.839%.
    - AES = from 62.436% to 65.956%.
    - DES = 62.753% to 66.352%.

The results showed a good performance in the proposed algorithm. Time it is measure of the time taken in encryption. The values showed no considerable change among the techniques. The results showed that the proposed algorithm has high measures of PSNR, SNR, and a good execution time. That means a highly secured and robust system.

The advantages of the proposed technique can be summarized as ; using chains to make high security, higher Peak Signal to Noise Ratio (PSNR) and its lower Absolute Mean Square error.

Moreover, it has been observed that the proposed algorithm achieved good results in all experiments with a high security and less time. The images used in this thesis are (Lena, pepper, and baboon) that can display the difference between the original images and encrypted images.

Finally, after comparing the related work with this study it was observed that the used technique in this study is more reliable due to the long secret key and its complexity and randomness.

5.2 Future Work

The proposed algorithm technique has been applied utilizing a computer network between a sender and a receiver. Both sides must use the same model to decrypt the image. For future, the proposed technique can be used in many applications and usages such as: Mobile network applications.

The proposed technique can be developed to generate a secret key with a different key size with different image blocks to expand its usages and withholds different attack methods. In addition, the algorithm can be developed to be used with different types of image formats, encrypt//decrypt videos.

5.3 Recommendations

Due to the features of the proposed algorithm technique some recommendations are suggested to be implemented such as: The ciphering method must be developed to include byte to byte encryption, and this method must be developed to be used in various applications such as whatsApp, twitter and other social media application.

References

Ahmad, S. Alam, K. M. R. Rahman, H., and Tamura, S. (2015). *A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets*. *In Networking Systems and Security (NSysS)*, ***2015 International Conference on***, 1-5

Al-Husainy M. (2012). *A Novel Encryption Method for Image Security*, ***International Journal of Security and Its Applications***, 6(1), 1-8

Auyporn, W. and Vongpradhip, S. (2015). *A Robust Image Encryption Method Based on Bit Plane Decomposition and Multiple Chaotic Maps.*

BaniYounes M. A. and Jantan, A. (2008). *Image Encryption Using Block-Based Transformation Algorithm IAENG*. ***International Journal of Computer Science***, 35.

Boneh, D. Di Crescenzo, G. Ostrovsky, R. and Persiano, G. (2004). *Public key encryption with keyword search. In Advances in Cryptology-Eurocrypt.* ***Springer Berlin Heidelberg,*** 506-522.

Chang, C. Hwang, M. and Chen, T. (2001). *A new encryption algorithm for image cryptosystems*, ***The Journal of Systems and Software*** 58, 83-91.

Delfs, H. and Knebl, H. (2007). *Symmetric-key encryption* Introduction to cryptography: principles and applications. ***Springer.***

Guo, J., Ling, S., Rechberger, C., and Wang, H. (2010). *Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. In Advances in Cryptology-ASIACRYPT 2010****, Springer Berlin Heidelberg****, 56-75*

Kaur, N. and Singh, H. (2012). *Efficient and Secure Data Storage in Cloud Computing Through Blowfish, RSA and Hash Function.* ***International Journal of Science and Research (IJSR),*** 4 (5)

Lindner, R. and Peikert, C. (2011). *Better key sizes (and attacks) for LWE-based encryption. In Topics in Cryptology–CT-RSA 2011*, ***Springer Berlin Heidelberg,*** 319-339

Microsoft Corporation all rights reserved. (2005), *Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements,* ***(WSE)*** 3.0

Reader, M. and Salam, K. (2014). *Image Encryption and Decryption Using Selective Block Encryption Technique*, ***International***

Journal of Computer Science & Engineering Technology (IJCSET), 5(09), 1-8.

Sathish, K. BhoopathyBagan, K. and Vivekanand, V. (2011). *A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems.* ***Procedia Computer Science,*** 3, 378–387.

Sivakumar, T. and Venkatesan, R. (2013). *A Novel Image Encryption Approach using Matrix Reordering.* ***WSEAS Transactions on Computers***, 12(11), 407-418.

Song, C. and Qiao, Y. (2015). *A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos*. ***Entropy,*** 17

Wadi, S. M. and Zainal, N. (2013). *Rapid Encryption Method Based on AES Algorithm for Grey ScaleHD Image Encryption. Procedia Technology*. ***4th International Conference on Electrical Engineering and Informatics, ICEEI,*** 11, 51–56.

Yang, G. Yu. Pan, Q. Sun, S. and PengXu. (2015). *Novel Image Encryption based on Quantum Walks.* ***Scientific Reports***, 5 (7784).

Yun-peng, Z. Wei, L. Shui-ping, C. Zheng-jun, Z. Xuan, N. and Wei-di, D. (2009). *Digital image encryption algorithm based on chaos and improved DES,* ***IEEE International Conference on Systems, Man and Cybernetics.***

Chen, G. Mao, Y. and Chui, C. K. (2004). *Design of Image Security System Based on Chaotic Maps Group system (A Novel Approach for Image Encryption using Dynamic SCAN Pattern* , ***International Journal of Computer Science*** 41, 2